



IRS Nationwide
TaxForum | 2019

Treasury Inspector General for Tax Administration (TIGTA):

**Helping You and Your Clients Steer
Clear of the Latest Frauds and
Swindles**

Learning Objectives

- Define TIGTA's role in protecting the integrity of tax administration;
- Differentiate between TIGTA's jurisdiction and that of the IRS;
- Discuss the various forms of preparer ethics and misconduct; and
- Discuss IRS impersonation scams and ongoing illicit Cyber activity targeting tax professionals.

What is TIGTA?

- Provides independent oversight of the IRS;
- Protects the integrity of Federal tax administration;
- Detects and prevents waste, fraud, and abuse; and
- Has three primary operating divisions:
 - Office of Investigations
 - Office of Audit
 - Office of Inspections and Evaluations

Office of Investigations

- Identifies and investigates IRS employee misconduct;
- Protects the IRS from external threats and corruption;
- Protects the integrity of IRS programs, operations, and critical infrastructure; and
- Detects and prevents waste, fraud, and abuse.

Recent TIGTA Audits

- Security of Taxpayer Data
 - *Actions Were Not Always Taken to Protect Taxpayers Associated With Reported External Data Breaches*
- Identity Theft
 - *Additional Actions Can Be Taken to Further Reduce Refund Losses Associated With Business Identity Theft*
- Improving Tax Reporting and Payment Compliance
 - *Taxpayers Generally Comply With Annual Contribution Limits for 401(k) Plans; However, Additional Efforts Could Further Improve Compliance*

Recent Inspections and Evaluations

- Virtual Service Delivery Program
 - *Although Virtual Face-to-Face Service Shows Promise, Few Taxpayers Use It*
- Offer in Compromise Public Inspection Program
 - *Management of the Offer in Compromise Public Inspection Program Continues to Be a Concern*

I.R.C. § 6103

- As a component of the Treasury Department with tax administration duties, TIGTA is bound by Title 26, United States Code Section 6103, the tax information confidentiality law; and
- Section 6103 prohibits the disclosure of tax returns or return information, except as authorized by an exception contained in the statute or as made public record in a tax administration proceeding.

Ethics and Integrity

(According to Webster's Dictionary)

- Ethics: A group of moral principles or set of values;
- Integrity: An uncompromising adherence to a code of moral, artistic, or other values; and
- MEANING: Always doing the right thing, even if no one is watching.

Circular 230

- Circular 230, also known as Subtitle A, Part 10 of Title 31 of the CFR;
- Sets forth rules under which tax preparers can represent clients before the IRS; and
- IRS's Office of Professional Responsibility (OPR) oversees most preparer conduct.

Preparer Misconduct

- False statements on IRS Forms 2848, *Power of Attorney and Declaration of Representative*; and

| | | | | |
|--|--|---|--|--|
| Form 2848 (Rev. July 2014) Department of the Treasury Internal Revenue Service | | Power of Attorney and Declaration of Representative <small>► Information about Form 2848 and its instructions is at www.irs.gov/form2848.</small> | | OMB No. 1545-0150 For IRS Use Only Received by: _____ Name _____ Telephone _____ Function _____ Date ____/____/____ |
| Part I Power of Attorney Caution: A separate Form 2848 must be completed for each taxpayer. Form 2848 will not be honored for any purpose other than representation before the IRS. | | | | |
| 1 Taxpayer information. Taxpayer must sign and date this form on page 2, line 7. | | | | |
| Taxpayer name and address Stan Doe 1040 Any Street Anytown, VA 22000 | | Taxpayer identification number(s) 000-00-0000 Daytime telephone number 000-000-0000 | | |
| hereby appoints the following representative(s) as attorney(s)-in-fact: 2 Representative(s) must sign and date this form on page 2, Part II. | | Plan number (if applicable) CAF No. 6800-06530R | | |
| Name and address | | CAF No. | | |

- Failure to disclose that preparer is disbarred or otherwise unauthorized to appear before the IRS.

Preparer Misconduct (Cont.)

- Sending e-mails or fabricating documents purporting to be from the IRS;
- Improper disclosure of a client's tax information; and
- Fraudulent levy releases.

Preparer Misconduct (Cont.)



Preparer Misconduct (Cont.)

Unauthorized disclosure of protected tax information



Payable

If you have a qualifying child, attach Schedule EIC.

67
68
69
70
71

Refund

72
73a
73b
73c
73d

Amount of line 71 is more than the amount on line 67. Subtract line 60 from line 71. This is the amount you want refunded to you. If Form 8888 is attached, check ☐ 8801 ☐ 8885

Routing number ☐ **Type:** ☐ Check

Preparer Misconduct Case #1

- **New Jersey Tax Preparer Sentenced in Scheme to Defraud the IRS and Clients**
- On December 21, 2018, in the District of New Jersey, tax preparer was sentenced in connection with a scheme to defraud the IRS and misappropriate his clients' monies by engaging in the filing of false tax returns and bank fraud
- Prepared or presented at least 21 fraudulent and false tax returns to the IRS for tax years 2009 through 2015, resulting in a loss to the IRS of approximately \$491,007
- Tax preparer was sentenced to 32 months' imprisonment, followed by five years' supervised release. He was further was ordered to forfeit \$61,000, pay \$499,997.72 in restitution , and pay a special assessment fee of \$800

Preparer Misconduct Case #2

- **New Jersey Accountant Pleads Guilty to Bribery of IRS Agent**
- On February 20, 2019, in the District of New Jersey, a Certified Public Accountant was charged with and pled guilty to bribery of an IRS revenue agent. Specifically, the CPA knowingly gave the revenue agent approximately \$3,000 to influence the outcome of an audit by reducing his client's tax liability
- The CPA offered a \$3000 payment to the revenue agent if the revenue agent could "help out" by reducing his client's tax liability.

Preparer Misconduct Case #3

- **Tax Preparer Charged for Using Customer Information in Scheme to Defraud**
- On March 13, 2019, in the District of Utah, a tax preparer was charged with wire fraud and aggravated identity theft in a scheme to defraud the IRS and financial institutions
- The tax preparer allegedly obtained the PII of customers and potential customers, as well as PII that had been stolen from individuals in burglaries, and used this information to create and file false tax returns, to alter and cash fraudulent checks, and to apply for fraudulent credit accounts
- If convicted, the tax preparer could face a maximum statutory sentence of 20 years' imprisonment for wire fraud, plus a mandatory two-year sentence for aggravated identity theft.

IRS Impersonation Scam

- Largest ever phone scam;
- Calls received by taxpayers in every State;
- Callers claim taxpayers owe taxes and must pay immediately; and
- Callers are aggressive and threatening.

IRS Impersonation Scam (Cont.)

- TIGTA is dedicated to educating the public to prevent fraud against the IRS and to protect taxpayers;
- PSAs are available on YouTube in English and Spanish; and
- “Advise and Disrupt” strategy created to help combat the impersonation scam.

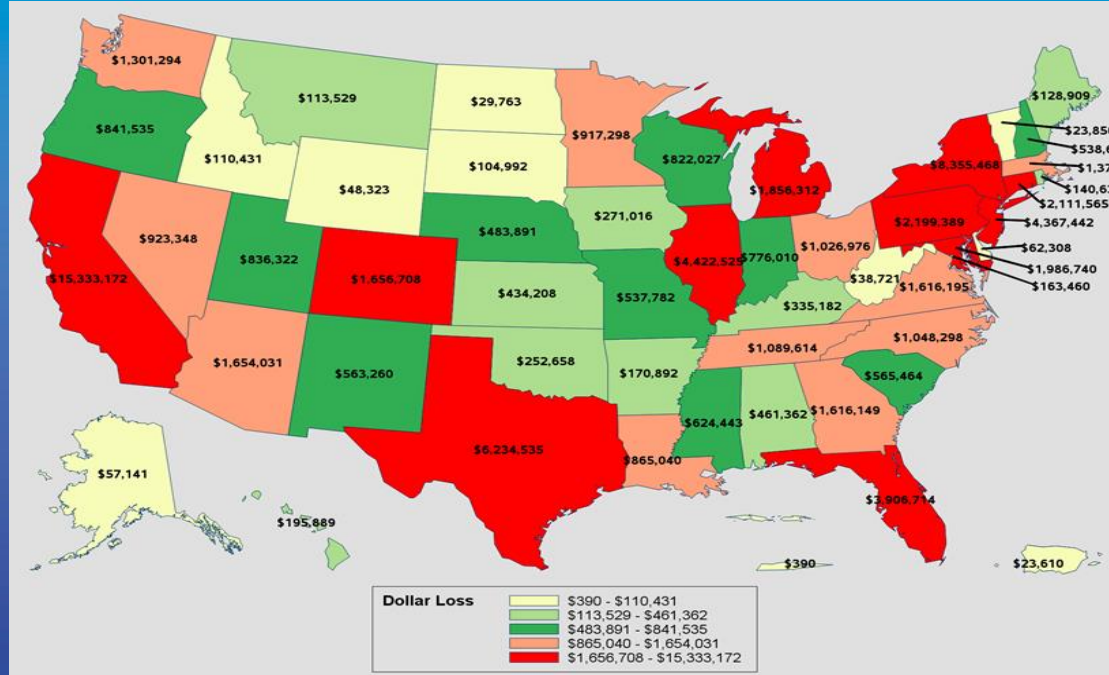
Traits of Scam Callers

- May know the information about the intended victim – such as digits of SSN, address, banking information;
- Spoof caller ID information to appear as if calling from the IRS; and
- Demand payment using a prepaid money card, including Green Dot[®], iTunes[®], MoneyGram[®], Western Union[®], or wire transfers.

Traits of Scam Callers (Cont.)

- May send bogus IRS e-mails to legitimize the scam; and
- Subsequent calls claiming to be the police, DMV, or the IRS to verify initial debt claims and confirm threatened legal action.

States Hardest Hit by Phone Scams



IRS Impersonation Scam Indictments

- April 2019: Indian National extradited to the United States to face charges for his role in a complex impersonation scam
- March 2019: Three individuals plus a business charged in IRS impersonation scam.
- November 2018: 1 indicted/arrested in GA.
- September 2018: 15 individuals and five India-based call centers indicted in GA. Approximately \$5.5 million and more than 4,000 victims.
- August 2018: 1 sentenced in PA to 234 months in prison and \$896,112.33 in restitution. Scheme spanned 18 States and perpetuated a stereotypical fear of a Government agency.
- June 2018: 1 arrested in MN. Approximately \$750,000. In possession of several hundred third-party gift cards at time of arrest.

IRS Impersonation Scam Indictments (Cont.)

- July 2018: 21 sentenced in TX. Cumulative prison time more than 174 years. The defendants were part of the October 2016 indictment of 56 individuals and five India-based call centers. Multiple schemes involving approximately \$272 million dollars of total fraud and more than 15,000 victims.
- April 2017: 10 individuals indicted in AR. The suspects travelled to 30 different States to collect money using approximately 80 different false identities. Approximately \$8.8 million from more than 7,000 victims.

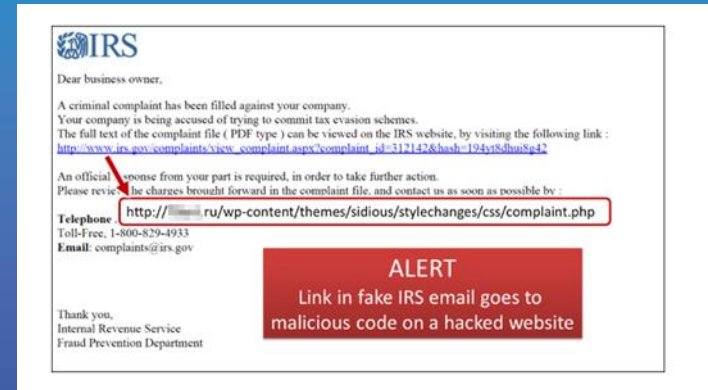
Other Impersonation Scams

“LOTTERY WINNING” Scams

- Jamaican resident sentenced in conspiracy to obtain money from elderly and vulnerable individuals in the United States and Canada;
- Purchased “client lists” of elderly and vulnerable individuals from brokers specializing in such information;
- Victims were told they had won millions of dollars in a lottery or sweepstakes, but must send payment for taxes and other fees before receiving winnings; and
- Sentenced to 63 months’ imprisonment and restitution totaling \$577,703.78.

Other Impersonation Scams (Cont.)

- False IRS websites
- Hyperlink on spam e-mail
- Phishing



Official IRS E-Mail?



Suspicious E-Mails

1. Forward the suspect e-mail(s) to **phishing@irs.gov**;
2. Delete it from your computer; and
3. **DO NOT** reply, open any attachments, or click on any links.

Victims of IRS Impersonation *(Phone or E-Mail Scams)*

- Call the IRS at 800-829-1040 *(if victim knows or thinks taxes are owed)*;
- Call the TIGTA Hotline at 800-366-4484 *(if victim knows no taxes are owed)*; and/or
- Contact bank if financial information given to scammer.

Reporting Scam Calls



TIGTA

Treasury Inspector General for Tax Administration

Promoting integrity in the administration of Internal Revenue laws

[Home](#)
[About TIGTA](#)
[Audit](#)
[Investigations](#)
[Inspections & Evaluations](#)
[Publications](#)
[Careers](#)
[Contact](#)

Hotline
Important Notices
Recovery Act
Treasury | IRS

► **LATEST IRS IMPERSONATION SCAM UPDATE: Do not use iTunes Gift Cards to pay your taxes...** [learn more.](#)

► If you believe you have been a victim of an IRS Impersonation Scam, [contact us.](#)

► View this [Public Service Announcement video.](#)

► Downloadable IRS Scam Files: [Warning Flyer](#), [5X8 Poster](#) & [11X17 Poster.](#)

► TIGTA partners with the Department of Justice's Elder Justice Initiative, view [webinar.](#)

► If you lost money to IRS scammers via Western Union, you may be able to file a claim to recover funds. Visit the [Federal Trade Commission's](#) website to learn more and get started.



SCAM ALERT

Meet the IG

An Inspector General Like No Other [video]

Latest Semiannual Report [PDF]

Latest Management Performance Challenges Facing the IRS [PDF]

Congressional Testimony

FY2018 Audit Reports

FY2018 Inspections & Evaluations Reports

Investigations Highlights

TIGTA Related Department of Justice Press Releases

No Fear Act

TIGTA Information Related to the American Recovery and Reinvestment Act of 2009

Recovery.gov

Whistleblower Protection Ombudsman

The Treasury Inspector General for Tax Administration (TIGTA) was established under the IRS Restructuring and Reform Act of 1998 to provide independent oversight of IRS activities. TIGTA promotes the economy, efficiency, and effectiveness in the administration of the internal revenue laws. It is also committed to the prevention and detection of fraud, waste, and abuse within the IRS and related entities.

 **Subscribe to Email Updates**

Enter Email Address

Recent Audit Reports

November 20, 2017
Processes Do Not Always Ensure That Electronic Filing Identification Numbers Are Assigned to Qualified Applicants or Deactivated When Required [PDF]
»Press Release

October 16, 2017
A Significantly Reduced Automated Substitute for Return Program Negatively Affected Collection and Filing Compliance [PDF]
»Press Release

October 10, 2017
The Internal Revenue Service...

Recent Investigations

December 28, 2017
California Psychiatrist Sentenced to Prison for Bribing an Internal Revenue Agent

December 28, 2017
Two Florida Men Plead Guilty to Money Laundering and Extortion Conspiracy Related to IRS Impersonation Scheme

December 28, 2017
Georgia Man Arrested in Refund Scheme Using Stolen Tax Information

December 28, 2017
South Florida Man Indicted on Charges of Conspiracy and Theft

IRS Impersonation Scam Reporting

Report Fraud, Waste, & Abuse

Whistleblower Retaliation Reporting

Contractor Fraud Reporting

FOIA

Jump to...

Search Site

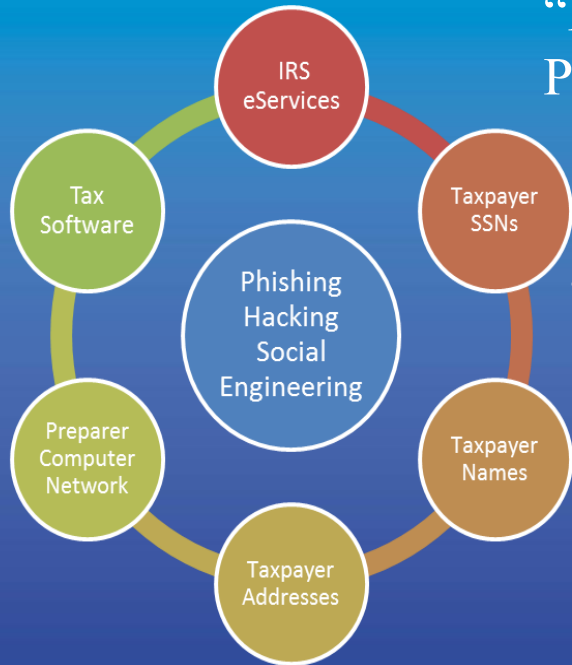
Readers & Viewers

pl?https://www.youtube.com/channel/UC4dSU08ElmzA_o7atb929AA

Cyber Targeting of Tax Preparers

“IRS, Security Summit Partners Warn Tax Professionals of high risk of data theft attacks”

- IRS Press Release IR-2018-245, December 7, 2018



“Consumer Alert: IRS Warns Taxpayers, Tax Pros of New e-Services Scam”

- IRS Press Release IR-2017-170, Oct. 11, 2017

The IRS today warned all e-Services users to beware of a new phishing scam that tries to trick tax professionals into “signing” a new e-Services user agreement. The phishing scam seeks to steal passwords and data.

Cyber Targeting of Tax Preparers

- 2018 Reports to the FBI Internet Crime Complaint Center
 - Business Email Compromise (BEC)
 - 20,373 victims with \$1.3 Billion in losses
 - Technical Support Fraud
 - 14,408 victims with \$38.7 Million in losses
 - Corporate Data Breaches
 - 2,480 victims with \$117.7 Million in losses

Cyber Targeting of Tax Preparers

- 2018 Reports to the FBI Internet Crime Complaint Center
 - Phishing/Vishing
 - 26,379 victims with \$48.2 Million in losses
 - Government Impersonators
 - 10,978 victims with \$64.2 Million in losses
 - Malware
 - 2,811 victims with \$7.4 Million in losses

Cyber Targeting of Tax Preparers

- Primary targets - Financial and personal information
 - On preparer's local computer network
 - In preparer software containing/processing PII
 - In preparer's IRS eServices account

Cyber Targeting of Tax Preparers

- Recent trends
 - Recent phishing email scams to harvest user account information
 - “Unlock” tax software accounts
 - Posing as state accounting or professional associations

Cyber Targeting of Tax Preparers

- Recent trends
 - Malicious software (Malware) designed to steal financial and network account passwords
 - Advanced cyber attacks against poorly secured networks
 - Ransomware designed to encrypt network devices
 - Attacker offers to send key to unencrypt for a fee

Cyber Targeting of Tax Preparers

- Indicators of trouble
 - Suspicious activity indicating compromise of local network
 - IRS eServices will show login history
 - Report dates showing login activity not made by you

Cyber Targeting of Tax Preparers

- Indicators of trouble
 - Unusual CAF activity
 - Take note of unauthorized Form 8821 or 2848s filed in your name
 - EFIN/PTIN activity higher than the number of returns you submitted
 - Can be viewed through eServices

Cyber Targeting of Tax Preparers

- Indicators of trouble
 - Customers receiving mailed, unsolicited tax transcripts from previous years
 - Customers receiving mailed notification of the establishment of an eAuthentication account which they did not create

Cyber Targeting of Tax Preparers

- Indicators of trouble
 - Tax software vendor (e.g. Drake, Intuit, etc) advises a fraudulent IRS document with your EFIN has been submitted to secure a software purchase

Cyber Targeting of Tax Preparers

- Reporting to TIGTA
 - Suspicious logons or activity on your eServices account not accomplished by you
 - Submission of fraudulent 8821/2848s to the IRS
 - Fraudulent IRS EFIN memos sent to software vendors
 - Customers who receive unsolicited transcripts or notices for IRS eAuthentication accounts they didn't create

Cyber Targeting of Tax Preparers

- Relevant IRS Publications
 - Publication 4557, Safeguarding Taxpayer Data
 - Publication 5293, Data Security Resource Guide for Tax Professionals
 - Publication 3112, IRS e-File Application and Participation
 - Publication 1345, Handbook for Authorized e-File Providers of Individual Tax Returns

How Can You Protect Federal Tax Administration?

- Report instances of tax preparer or IRS employee misconduct;
- Report allegations of potential risks to IRS employee safety; and
- Warn taxpayers about phone scams.

How to Contact TIGTA

E-mail: complaints@tigta.treas.gov



Telephone: 1-800-366-4484



Internet: <http://www.tigta.gov>



Questions?

E-mail: complaints@tigta.treas.gov

Telephone: 1-800-366-4484

Internet: <http://www.tigta.gov>

